



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHIED	33012/274/10	4721
5909	7590	08/31/2004	EXAMINER	
NAWROCKI, ROONEY & SIVERTSON SUITE 401, BROADWAY PLACE EAST 3433 BROADWAY STREET NORTHEAST MINNEAPOLIS, MN 554133009			WASSUM, LUKE S	
			ART UNIT	PAPER NUMBER
			2177	

DATE MAILED: 08/31/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/448,154	Applicant(s) GERMSCHIED ET AL.	
	Examiner Luke S. Wassum	Art Unit 2177	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 June 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 April 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. The Applicants' amendment, filed 24 June 2004, has been received, entered into the record, and considered.
2. As a result of the amendment, claims 1, 3, 5-8, 11, 13, 16 and 19 have been amended.
Claims 1-20 remain pending.

The Invention

3. The claimed invention is an apparatus for and method of using an Internet terminal coupled to the World Wide Web to access an existing proprietary database management system, wherein said accessing does not require the transmission of a user identifier across the Internet, thereby enhancing security. Sign in information from a user (such as a user id and password) is processed only at the Internet terminal, and only a special field indicative of the site specific user validation data is transmitted over the Internet as part of the service request.

Specification

4. In view of the amendment to the specification, the examiner withdraws the pending objection to the specification.
5. Applicant has incorporated by reference numerous co-pending applications at various points in the specification. Examiner notes that incorporation by reference of an application in a printed United States Patent constitutes a special circumstance under 35 U.S.C. § 122 warranting that access

of the original disclosure of the application be granted. The incorporation by reference will be interpreted as a waiver of confidentiality of only the original disclosure as filed, and not the entire application file. See *In re Gallo*, 231 USPQ 496 (Comm'r Pat. 1986).

If Applicant objects to access to the entire application file(s), two copies of the information incorporated by reference must be submitted along with the objection. Failure to provide the material within the period provided will result in the entire application(s) (including prosecution) being made available to petitioner. The Office will not attempt to separate the noted materials from the remainder of the application. See *In re Marsh Engineering Co*, 1913 C.D. 183 (Comm'r Pat. 1913).

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

8. Independent claims 1, 6, 11 and 16 cite limitations whereby a user is validated at an Internet terminal through the entry of a user identifier and password, and wherein the Internet terminal contains a site-specific terminal identifier. Said terminal identifier (but not the user-specific user identifier) is transmitted to a remote database management system as part of a service request. At

the remote database management system, the terminal identifier is compared with a security profile associated with a command script that would satisfy the service request, and if compatible, the command script is executed in order to satisfy the service request and to transmit the requested information to the Internet terminal.

In the Applicants' arguments regarding the claim rejections under 35 U.S.C. § 112, first paragraph, it is stated that "...transfer of the terminal identifier is required [for submission of a secure service request], even though the transfer of the user identifier is not. Comparison between the terminal identifier and security profile results in honoring or denial of the requested service." Thus it seems plain that the operation of the system regarding the terminal identifier is central to the claimed invention.

Also important to the invention is the User Validation Service, which is the mechanism whereby the user identifier at the Internet user terminal is converted to a terminal identifier (see specification, page 7, lines 9-16).

The Applicants state in their response to the last Office action that "The detailed description of the creation and honoring of the "terminal identifier" is found within Figs 14-15 of the disclosure." (see page 11, middle).

The examiner assumes that the Applicants intended to cite Figures 13 and 14, as there is no Figure 15 in the application.

Figure 13 illustrates a number of software method calls, disclosing only the names of the methods and the arguments passed. The entire detailed disclosure in the specification concerning Figure 13 is as follows:

"Fig. 13 is a class diagram showing creation of a site security profile."

Figure 14 illustrates a number of 'messages' and descriptions. The entire detailed disclosure in the specification concerning Figure 14 is as follows:

"Fig. 14 is a listing of messages associated with creation of a site security profile."

Both Figures 13 and 14 consist largely of program module calls and citations of class names, for the most part quite cryptic, and the examiner finds that these drawing figures do little or nothing to convey to one of ordinary skill in the art the information necessary to implement the claimed system. Given the central role of the terminal identifiers and the User Validation service through which they are created and managed, and in view of the lack of detailed disclosure regarding them, the examiner finds the claims non-enabled.

9. Dependent claims 2-5, 7-10, 12-15 and 17-20, incorporating the deficiencies of their respective parent claims, are likewise rejected.

10. Regarding the Applicants' remarks regarding the rejections of claims 1-20 under 35 U.S.C. § 112, second paragraph, it is assumed by the examiner that in the disclosure on page 34, last paragraph, that "...the service handler 322 requests the user to provide a user-id...", the 'user-id' refers to the terminal identifier discussed in said remarks. Assuming this is the case, and contingent upon an amendment to the specification clarifying this fact, the examiner withdraws these rejections.

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2177

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

13. Claim 1 recited the limitation that the second user identifier has a format "similar" to said first user identifier. The use of the term "similar" renders the claim indefinite, since it fails to define the limitation to a sufficient degree as to allow an ordinarily skilled artisan to determine the meets and bounds of patent protection sought by the Applicants, nor is the meaning of what constitutes a "similar format" disclosed in the specification.

14. Claim 2 recites the limitation "said site specific security profile" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

17. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

18. Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175).

19. Regarding claim 1, **Garrison** teaches a data processing environment having a user with a user identifier which uniquely identifies said user at a terminal at a particular site which generates a service request requesting access to secure data responsively coupled via a publicly accessible digital data communication network to a database management system having at least one database

containing said secure data as claimed, comprising a security profile whereby said database management system permits said terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect

all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches a data processing environment wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches a data processing environment wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since this allows a system to provide pre-defined data requests that can be accessed by a client terminal at the touch of a button, rather than requiring said client terminal to manually format such a request (see **Steele et al.**, col. 7, lines 33-56).

20. Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

- a) a terminal located at a particular location (see col. 4, lines 1-32) having a user with a user identifier which identifies said user (see col. 6, line 60 through col. 7, line 13);
- b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32); and

- c) a security profile generated by said database management system whereby said database management system provides access to a particular secure portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect

all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches an apparatus wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches an apparatus wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since this allows a system to provide pre-defined data requests that can be accessed by a client terminal at the touch of a button, rather than requiring said client terminal to manually format such a request (see **Steele et al.**, col. 7, lines 33-56).

21. Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal having a user with a user identifier located at a site to securely access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

- a) signing on to said terminal by said user utilizing said user identifier (see col. 2, line 64 through col. 3, line 2, disclosing that the client transmits a password to the client to

- identify the user of the client system, meaning that the user has necessarily signed on to the client system utilizing a user identifier);
- b) transmitting a service request requiring secure access to said database from said terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);
 - c) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);
 - d) determining a security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);
 - e) comparing said security profile with said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and
 - f) honoring said service request if and only if said service request corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches a method wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches a method wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since this allows a system to provide pre-defined data requests that can be accessed

Art Unit: 2177

by a client terminal at the touch of a button, rather than requiring said client terminal to manually format such a request (see **Steele et al.**, col. 7, lines 33-56).

22. Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

- a) means located at a site for permitting a user having a user identifier to interact with a database responsively coupled via a publicly accessible digital data communication network (see col. 4, lines 1-32);
- b) means responsively coupled to said permitting means via said publicly accessible digital data communication network for offering data processing services involving access to said database in response to said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and
- c) means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile wherein said security profile permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data

communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches an apparatus wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches an apparatus wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since this allows a system to provide pre-defined data requests that can be accessed by a client terminal at the touch of a button, rather than requiring said client terminal to manually format such a request (see **Steele et al.**, col. 7, lines 33-56).

23. Regarding claim 2, **Garrison** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

24. Regarding claims 3, 8, 12, 13 and 18, **Garrison** additionally teaches an improvement, method and apparatus further comprising a portion of a service request whereby said database management system receives an identifier corresponding to said particular site (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

25. Regarding claims 4, 14 and 17, **Garrison** additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

26. Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said terminal accesses said data entity by transferring a service request to said system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

27. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175) as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("UNISYS CSG MarketPlace – The Mapper System").

28. Regarding claims 5 and 19, **Garrison**, **De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison**, **De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is a legacy database management system.

However, **Unisys** teaches the database management system MAPPER, constituting a legacy database management system (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

29. Regarding claims 9 and 15, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches the database management system MAPPER (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

30. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

31. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

32. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in

Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175) as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("Why Do I Need Cool ICE?").

33. Regarding claims 5 and 19, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is a legacy database management system.

However, **Unisys** teaches a system wherein the database management system used is MAPPER, constituting a legacy database management system (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

34. Regarding claims 9 and 15, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches a system wherein the database management system used is MAPPER (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

35. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

36. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

Response to Arguments

37. Applicant's arguments filed 24 June 2004 have been fully considered but they are not persuasive.

38. The Applicants argue that the examiner's rejection of claims 1-20 under 35 U.S.C. § 112 first paragraph is improper. The examiner respectfully disagrees.

The Applicants have amended the independent claims in response to the claim rejections, attempting to define a 'terminal identifier' which has a format similar to that of the user identifier as the mechanism whereby information is transferred across the Internet in order to validate a user's service request as being authorized. However, as detailed above, in view of the lack of detailed disclosure of the mechanism for defining and managing the claimed terminal identifier (the extent of the detailed disclosure within the specification that is concerned with the claimed security system is limited to the summary of the invention, pages 7-9, and the discussion of Figure 10, pages 33-34), and also the fact that the term 'terminal identifier' is not used in the specification, the claims are not enabled by the disclosure to a sufficient degree to allow an ordinary artisan to make and use the invention.

Further exacerbating the enablement problem are several seemingly contradictory statements in the specification. For instance, on page 7, lines 12-16, it is disclosed that each site must implement a User Validation service, which converts site-specific data to a valid UserID/Password. However, the following paragraph at lines 17-20 disclose that the User Validation service provides the capability for the browser (presumably at the site) to send (presumably to the server) information

(the Validation Service-generated UserID/Password?), which is then translated into a UserID/Password on the Cool ICE Web Application server. "This bypasses the need to send a UserID/Password from browser to server, which enhances security."

The examiner assumes that the confusion stems from inconsistent use of terminology across the specification and the claims. The User Validation service presumably converts a user-specific UserID/Password (the 'site-specific data' on page 7, line 12) to a terminal identifier (as identified by the claims, but which is disclosed as a 'valid UserID/Password' on page 7, line 13) and then transmits this terminal identifier (now disclosed as 'information' at page 7, line 17) from the user's web browser to a server, where it is disclosed at page 7, line 18 that it is translated into a UserID/Password on the server.

In contrast with the above analysis, the specification discloses on page 34, last paragraph, that when it is determined at the server that a service request is associated with a security profile, "the service handler requests the user to provide a user-id via ... World Wide Web", and awaits a response via the World Wide Web. Even if the 'user-id' cited here is the claimed terminal identifier, there is still an inconsistency. The Summary of the Invention, the Abstract, and the claims all state that the 'special field' (Abstract)/terminal identifier (claims)/information (page 7, lines 17-18) is transmitted as part of the service request, but the disclosure of page 34 states that the terminal identifier is not transmitted until the service request has arrived at the server, a determination is made that the service request has an associated security profile, and the service handler sends a request back to the user to provide a user-id (page 34, last paragraph).

39. The Applicants argue that the rejection of claims 1-20 under 35 U.S.C. § 112, second paragraph is improper.

The examiner has found these arguments persuasive, contingent upon clarifying amendments made to the specification as outlined above in paragraph 10 of this Office action.

40. The Applicants argue that the **De Capitani di Vimercati et al.** reference teaches away from the claimed invention. The examiner respectfully disagrees.

The Applicants cite three passages from the reference, as well as the caption on Table 1 as supporting the allegation that the reference teaches away from the claimed invention.

By way of introduction, the examiner first points out that nonpreferred embodiments of a disclosure constitute prior art. MPEP §2123 states:

NONPREFERRED EMBODIMENTS CONSTITUTE PRIOR ART

Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994) (The invention was directed to an epoxy impregnated fiber-reinforced printed circuit material. The applied prior art reference taught a printed circuit material similar to that of the claims but impregnated with polyester-imide resin instead of epoxy. The reference, however, disclosed that epoxy was known for this use, but that epoxy impregnated circuit boards have "relatively acceptable dimensional stability" and "some degree of flexibility," but are inferior to circuit boards impregnated with polyester-imide resins. The court upheld the rejection concluding that applicant's argument that the reference teaches away from using epoxy was insufficient to overcome the rejection since "Gurley asserted no discovery beyond what was known in the art." 27 F.3d at 554, 31 USPQ2d at 1132.).

In this case, the contents of Table 1 disclose a number of problems to be solved and possible solutions. Since these solutions are disclosed as possible, the examiner believes that they constitute prior art.

Furthermore, the three passages cited by the Applicants refer to authentication and access control *to the federation*, not to individual databases within the federation. In the second paragraph of section 2.1 Authentication and Access Control, page 88, this fact is recited:

"A first decision to be taken concerns whether users should connect and authenticate themselves to the federation in order to access federated data."

It is in this context that the reference concludes "Let us therefore assume that each user needs to identify himself to the federation." This is analogous to the claimed first user identifier uniquely identifying a specific user. The concept is that a user must be authenticated within the federation before access control at a local component can be considered.

Now that the reference has concluded that a user must identify himself to the federation, the next issue can be considered:

"The question that arises now is what happens when his requests are forwarded to the local sites. What identity should each local site consider, i.e., against whose authorizations should the local site enforce access control?" (page 89, first column, last paragraph).

The reference considers two different possibilities, summarized in the 'Authentication: Local Components' problem in Table 1. The users can be required to identify themselves at the site (local authentication), or the site can trust the identities as communicated by the federation (global authentication). If local authentication is to be applied, the user will have to type in login and password for each site involved in the transaction (see page 90, first column, first paragraph). If

global authentication is applied, "...a user's identity (and/or other information needed for access control) is passed to the site by the federation together with the request." This is identical to the method of authentication as is being claimed by the Applicants.

Finally, in section 3.2 Authentication, and particularly on page 95, first column, first paragraph, the reference teaches the *exact* authentication method claimed by the Applicants:

"For example, subject pattern **@site1* indicates all user identifiers at site1...For example, an authorization can specify that all users connecting to the federation from site site4 can execute certain operations."

And in the next paragraph...

"In the global authentication, federation's users do not need to identify themselves at the site, their identity as communicated to the site by the federation will be used for access control."

These disclosures are fully consistent with the claimed invention, and do not teach away from said invention. The examiner thus maintains the rejection of claims 1-20.

41. The Applicants also argue that the rejections of claims 5, 9, 10, 15, 19 and 20 are improper as having no motivation for the combination of references and that they teach away from the combination. However, besides the allegations themselves, there are no supporting arguments.

The examiner respectfully disagrees. The reasons motivating the combinations of the references are set out in the rejections of record, and in the view of the examiner are sufficient as to constitute a *prima facie* case on obviousness. The rejections are maintained.

PTO Relocation

42. Applicant(s) should be aware that the examiner is currently scheduled to move to the new Alexandria campus in late October 2004. At that time, the examiner's telephone number will be changed to (571) 272-4119. The new Tech Center 2100 main telephone number will be (571) 272-2100.

Conclusion

43. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hanson et al. (U.S. Patent 6,697,835) teaches a method for high speed parallel execution of multiple points of logic across heterogeneous data sources.

Germesheid et al. (U.S. Patent 6,751,618) teaches a method for a web application server to upload multiple files and invoke a script to use the files in a single browser request.

Hildebrandt et al. ("User Authentication in Multidatabase Systems") teaches the foundations and prerequisites for architectures of authentication in multidatabase systems.

44. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on

Art Unit: 2177

the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

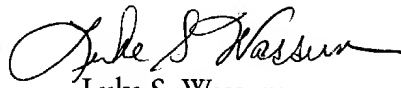
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 703-305-5706. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 703-746-5658.

Customer Service for Tech Center 2100 can be reached during regular business hours at (703) 306-5631, or fax (703) 746-7240.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Luke S. Wassum
Art Unit 2177